BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 31-1

28 OCTOBER 2011

Security

INTEGRATED DEFENSE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A7SO

Certified by: AF/A7S
(Brig Gen Jimmy E. McMillian)

Supersedes: AFPD31-1, 7 July 2007;
AFPD31-2, 10 April 2009

Pages: 13

This Air Force Policy Directive (AFPD) establishes the framework for how the Air Force formulates and applies Integrated Defense (ID). This Directive applies to all military and civilian Air Force personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. This Directive implements Department of Defense (DoD) Directive (DODD) 3025.13, *Employment of Department of Defense Resources in Support of the United States Secret Service*; DODD 3150.3, *Nuclear Force Security and Survivability*; DoD Instruction (DODI) 3224.3, *Physical Security Equipment (PSE) Research, Development, Test and Evaluation (RDT&E)*; DODI 5200.08, *Security of DoD Installations and Resources;* DODI 5100.76, *Safeguarding Conventional Arms, Ammunition, and Explosives (AA&E), The AA&E Physical Security Review Board;* DODD 5200.31, *DoD Military Working Dog (MWD) Program;* DODD 5210.41, *Security Policy for Protecting Nuclear Weapons;* DODD 5210.56, *Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence;* DoDI 6055.17, *Installation Emergency Management Program; and* DTM 09-012, *Interim Policy Guidance For DoD Physical Access Control.* This Directive interfaces with AFDD 3-10, *Force Protection*, AFDD 3-27, *Homeland Operations*, and joint doctrine contained in the Joint Publication 3-10, *Joint Security Operations in Theater*. This Directive issues overarching policy on conducting ID operations in order to sustain air, space, and cyberspace operations. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/rims.cfm**. Refer recommended changes and questions

about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

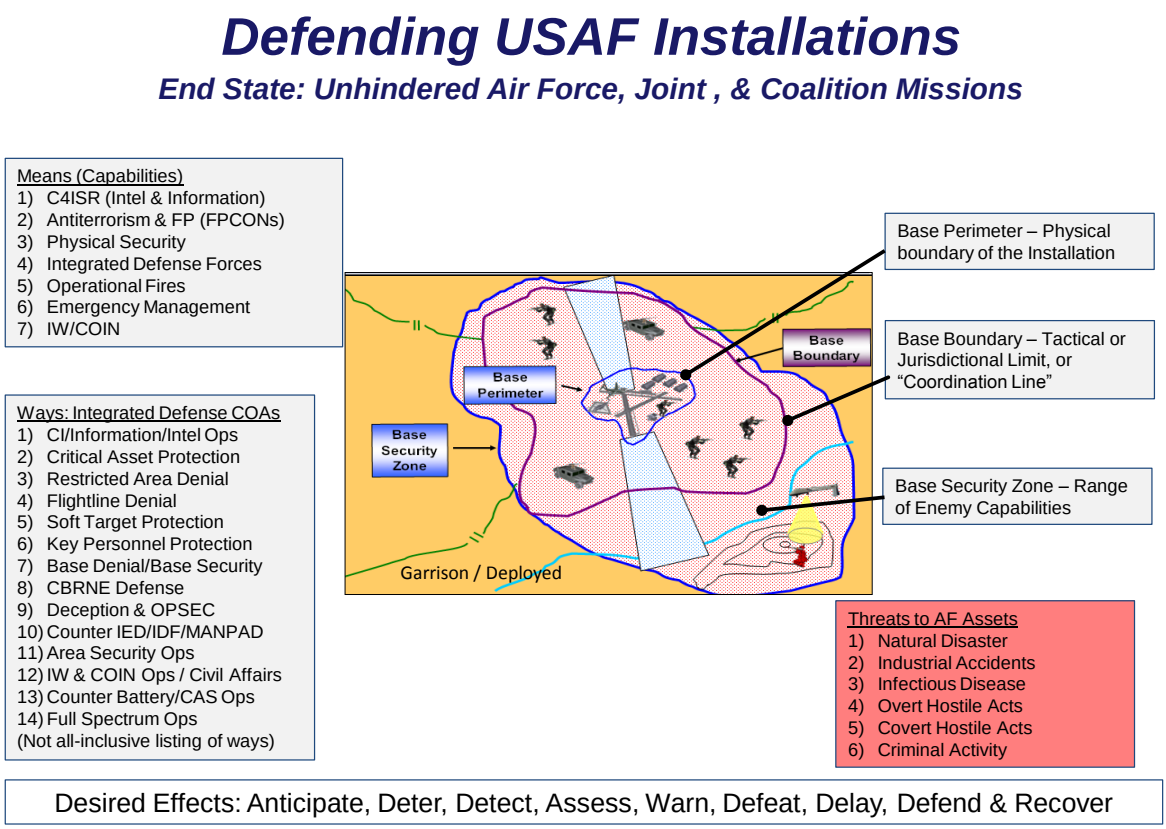
This document is substantially revised and must be completely reviewed. Consolidates and replaces AFPD 31-1, *Integrated Defense (ID)*, and AFPD 31-2, *Air Provost Operations*. This revision further solidifies the responsibilities of the Installation Commander in protecting and defending Air Force installations, personnel, and resources. An expanded list of references, abbreviations, acronyms, and terms (Attachment 1) is attached.

1. Air, space and cyberspace power projection assets are critical enablers to the national security of the United States and contribute to the achievement of national strategy objectives**.** A central and fundamental component of the Air Force capability is the power projection platform from which we operate, our installations and, their most important critical enabler, our professional Airmen. Both require a deliberate and focused security strategy for protecting and defending air, space, and cyberspace power, one that considers mission accomplishment, threats, vulnerabilities, and the inherent risks associated with operation of a military installation. Within the Air Force, that strategy is Integrated Defense (ID).

2. Protecting and defending Air Force Installations is a strategy; an end, means, ways construct, that employs a number of Air Force capabilities in a variety of ways to produce desired effects in the base defense battle space. This strategy, as depicted in Figure 1, leverages assigned AF resources against adaptive threats to protect Air Force resources and personnel. It is an Installation Commander's inherent responsibility to identify risks and develop risk management strategies to produce effects-based, integrated defense plans to ensure unhindered Air Force, Joint and Coalition missions.

3. ID is the integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations within the Base Boundary (BB) and the Base Security Zone (BSZ). These threats include, but are not limited to, terrorists, insiders, foreign intelligence and security services (FISS) and criminals. It is critical to integrate ID efforts with other Air Force capabilities to achieve synergistic effects using an all-hazards approach. Potential hazards to an installation include, but are not limited to, Chemical Biological Radiological Nuclear-High Yield Explosive (CBRNE) attacks, natural and man-made disasters, major accidents, and accidental or deliberate release of hazardous materials, toxic industrial materials or chemicals.

Figure 1. Integrated Defense (ID) Concept.



4. Installation commanders have a wide variety of capabilities available to accomplish ID. The capabilities (means) associated with ID include but are not limited to: Command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), weather, Antiterrorism & Force Protection Conditions (FPCONs), Physical Security, Integrated Defense Forces, Operational Fires, Emergency Management, and Irregular Warfare/Counterinsurgency (COIN) capabilities. Each of these capabilities is critical to ensuring unhindered Air Force, Joint, and Coalition operations in all environments from CONUS/OCONUS to austere deployed locations.

5. The integration of multiple Air Force capabilities within the Military Decision Making Process helps facilitate Course of Action (COA) development focused on achieving specific desired effects designed to protect and defend critical assets necessary to meet the commander's intent.

6. The nine ID Desired Effects are: Anticipate, Deter, Detect, Assess, Warn, Defeat, Delay, Defend, and Recover. Ideally, intelligence enables Commanders to anticipate threats and hazards as the first step in protecting and defending an installation. Commanders will identify additional ID effects to enable planning and course of action development. Installation Commanders will publish the desired effects in a Commander's Intent and mission statement.

7. ID COAs (ways) must comply with applicable laws and regulations. The laws, customs and culture, Status of Forces Agreements, Rule of Engagement, and Law of Armed Conflict in some

areas of operation may impose constraints and restrictions on ID operations. Therefore installations must work to synchronize ID efforts with friendly forces operating within the BSZ.

8. Commanders require timely and credible information and/or intelligence to protect their forces and make ID operations decisions. The synchronization of information will be executed through the Information Fusion Cell (IFC) IAW Air Force policy and guidance and tactics, techniques, and procedures.

9. Communications with and dispatch of ID Forces is conducted from the Base Defense Operations Center which is a part of the base Emergency Communications Center. Command and Control of ID Forces will be conducted IAW Air Force Incident Management System (AFIMS).

10. Roles and Responsibilities.

10.1. Commanders at all levels will:

10.1.1. Be responsible for executing assigned missions in the installation's ID plan.

10.1.2. Organize, train, and equip appropriate forces to conduct and sustain assigned ID operations.

10.2. AF/A1 will:

10.2.1. Provide guidance to MAJCOM/A1M on validating Security Forces manpower based on Security Forces Capability-based Manpower Standards.

10.2.2. Provide policy and guidance for integrating and vetting new/emerging institutional education and training requirements or learning outcomes into accessions, professional military education and ancillary training.

10.3. AF/A2 will:

10.3.1. Provide operational, planning, programming and budgeting guidance for AF intelligence support to ID operations.

10.3.2. Provide guidance supporting intelligence preparation of the operational environment (IPOE) and other threat information and staff estimates to support Installation Commanders' ID operations.

10.3.3. Provide collection management for ISR assets to support ID operations within the BSZ.

10.4. AF/A3/5 will:

10.4.1. Approve the Protection Level (PL) of Air Force assets.

10.4.2. Oversee development of homeland defense and civil support and Counter-Chemical, Biological, Radiological, and Nuclear (C-CBRN) doctrine, policy and operational standards, as outlined in AFPD 10-8, *Homeland Defense and Civil Support*, and AFPD 10-26, *Counter-Chemical, Biological, Radiological and Nuclear Operations.*

10.4.3. Develop doctrine, policy, standards and requirements for environmental threat and hazard information.

10.5. AF/A4/7 will:

10.5.1. Oversee the training, organizing, and equipping of personnel for all facets of Logistics, Installations, and Mission Support for ID.

10.5.2. Ensure Agile Combat Support, sustainment, and readiness through planning, programming and budgeting.

10.5.3. Establish implementation guidance for ID.

10.5.4. Integrate Air Force policy pertaining to protection and defense against all threats and hazards to Air Force Installations.

10.5.5. Through the AF/A7S, develop sustainment, planning, programming, training, integration and guidance for effects-based ID capabilities.

10.5.6. Through the AF/A7S, manage integration of ID Forces capabilities into AF, Joint, and Coalition, planning and operations.

10.5.7. Through the AF/A7S, manage ID risk management methodology and approaches.

10.5.8. Through the AF/A7C, provide field expertise, recommendations, support and other input for structural, environmental, Fire Emergency Services, Explosive Ordnance Disposal (EOD), Emergency Management (EM), and other engineer areas of expertise.

10.5.9. Ensure the AF/A7C develops engineer-related force protection (FP) and ID training standards and equipment requirements.

10.5.10. Through the AF/A7C, implement non-medical C-CBRN passive defense and consequence management programs as part of the EM program.

10.5.11. Ensure the AF/A7S determines minimum system security standards. Advocate MAJCOM, AFRC, and ANG manpower, facilities, and equipment requirements for conducting in-garrison and expeditionary ID operations.

10.5.12. Ensure the AF/A7S approves Air Force ID technology and equipment.

10.5.13. Through the AF/A7S, establish and interpret policy and oversee Air Force Law and Order Programs.

10.5.14. Develop, and coordinate with AF/A1D approval to integrate institutional education and training requirements, i.e. ancillary training, Professional Military Education, and accessions into the appropriate venues in support of ID operations prior to levying on the Total Force. NOTE: Career field specific requirements will be coordinated with the respective career field manager and/or Functional Authority Force Development for integration into the Career Field Education Training Plan and Course Training Standard as appropriate.

10.5.15. Provide cost and justification information to the DoD Physical Security Equipment Action Group (PSEAG) in support of program budgeting and execution.

10.5.16. Designate an individual to represent the Department of the Air Force in the DoD PSEAG.

10.5.17. Through the AF/A7S, provide use of Explosive Detection Dog (EDD) Teams to support the United States Secret Service (USSS).

10.5.18. Ensure the AF/A7S designates the DoD program manager for all matters pertaining to training of DoD military working dogs.

10.5.19. Ensure the AF/A7S coordinates with Undersecretary of Defense (Intelligence) (USD(I)) on development of policy for proper employment of EDD teams in support of the USSS.

10.5.20. Through the AF/A7S, provide the DoD Physical Security Review Board with incident information relating to conventional arms, ammunition and explosives (AA&E) and provide support to USD(I) for task groups related to safeguarding AA&E.

10.5.21. Through the AF/A7S, direct development of policy pertaining to arming of ID forces.

10.5.22. Ensure the AF/A7S coordinates with the USD(I) on the security of DoD installations and resources.

10.6. AF/SG will:

10.6.1. Develop medical-related FP and ID training standards and equipment requirements.

10.6.2. Provide field expertise, recommendations, support and other input for medical emergency management, medical CBRN operations and other medical areas of expertise.

10.7. SAF/IG will:

10.7.1. Ensure AFOSI provides Installation Commanders and Defense Force Commanders (DFCs) applicable counterintelligence (CI) information within the BSZ.

10.7.2. Ensure AFOSI establishes an effective liaison with host nation and civilian intelligence, security, and law enforcement agencies.

10.7.3. Ensure AFOSI maintains the capability to respond to criminal activities in support of law enforcement operations.

10.7.4. Ensure AFOSI provides immediate, worldwide, complementary support to the deployed area commanders by conducting specialized CI, counter-threat, and protective service operations.

10.8. MAJCOMs and ANG will:

10.8.1. Develop guidance and procedures in support of installation ID operations.

10.8.2. Program and budget resources to organize, train, and equip ID forces in support of installation ID operations.

10.9. Installation Commanders will:

10.9.1. Minimize mission degradation from threat activity within the BB and coordinate necessary support within the BSZ when the BSZ is not congruent with the BB; minimize loss of life and injury from threat activity and natural events; and protect government property and personnel from natural disasters, hostile and criminal acts.

10.9.2. As the Integrated Defense Risk Authority, assume identified risk for assigned, attached or transient DoD personnel and assets.

10.9.3. Ensure an organic capability exists to continuously fuse all-source FP information and deliver force protection intelligence (FPI) in support of ID.

10.9.4. Consider the potential effects produced by the threat/hazard, not just the nature of the threat/hazard.

10.9.5. Ensure Installation Commander's Intent and risk tolerance level is known and incorporated into local plans and instructions.

10.9.6. Ensure the DFC appropriately coordinates, assigns and tasks the Integrated Defense Force.

10.9.7. Ensure ID operations are synchronized with the appropriate Battle Space Owner (BSO).

10.9.8. Establish and maintain appropriate Support Agreements (SA) with local, regional and state civil authorities, private sector organizations and other federal facilities to address local support that either party might provide for immediate response to emergencies. When developing SAs, Commander's will ensure that Air Force commitments are consistent with relevant regulatory and statutory requirements, including specific funding authority.

11. Commanders of nuclear capable installations must plan and execute nuclear weapon security operations in accordance with DoD S-5210.41-M, *Nuclear Weapon Security Manual*, and AFMAN 31-108, Volumes 1-3, *Air Force Nuclear Weapons Security Manual* supplement.

MICHAEL B. DONLEY
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD O-2000.8-H, *DoD Antiterrorism Handbook,* February 1, 2004

DoD Directive 3025.13, *Employment of Department of Defense Resources in Support of the United States Secret Service,* September 13, 1985

DoD Directive 3150.3, *Nuclear Force Security and Survivability (S2),* March 8, 2004

DoD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, January 7, 2009

DoD Directive 5200.31, *DoD Military Working Dog (MWD) Program,* March 29, 2006

DoD Directive 5210.56, *Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties,* November 1, 2001

DoD Directive 5240.1, *DoD Intelligence Activities*, August 22, 2007

DoD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,* December 1982

DoD Directive 5525.5, *Department of Defense Cooperation with Civilian Law Enforcement Officials,* December 20, 1989

DoD Instruction 2000.16, *DoD Antiterrorism Standards,* December 8, 2006

DoD Instruction 3224.03, *Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E),* October 1, 2007

DoD Instruction 5030.34, *Agreement Between the United States Secret Service and the Department of Defense Concerning Protection of the President and Other Officials,* September 17, 1986

DoD Instruction 5100.76, *Safeguarding Conventional Arms, Ammunition, and Explosives (AA&E) and the AA&E Physical Security Review Board*, October 8, 2005

DoD Instruction 5200.08, *Security of DoD Installations and Resources,* December 10, 2005

DoD Instruction O-5210.63, *DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials,* November 21, 2006

DoD Instruction 6055.17, *Installation Emergency Management Program,* January 13, 2009

DoD 5200.08-R, *Physical Security Program,* April 9, 2007

DoD S-5210.41-M, *Nuclear Weapon Security Manual*, July 13, 2009

Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms,* October 31, 2009

Joint Publication 3-0, *Joint Operations,* March 22, 2010

Joint Publication 3-07.2, *Antiterrorism,* April 14, 2006

Joint Publication 3-10, *Joint Security Operations in Theater,* February 3, 2010

Joint Publication 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear Environments,* August 26, 2008

Joint Publication 3-27, *Homeland Defense,* July 8, 2007

Joint Publications 3-40, *Combating Weapons of Mass Destruction*, June 10, 2009

AFDD 1, *Air Force Basic Doctrine,* 17 November 2003

AFDD 2-3, *Irregular Warfare,* 1 August 2007

AFDD 2-4, *Combat Support*, 23 March 2005

AFDD 3-10, *Force Protection,* 9 November 2004

AFDD 3-27, *Homeland Operations*, 21 March 2006

AFDD 3-40, *Counter-Chemical, Biological, Radiological, and Nuclear Operations*, 17 September 2010

AFPD 10-4, *Operations Planning, Air & Space Expeditionary Force Presence Policy*, 30 April 2009

AFPD 10-8, *Homeland Defense and Civil Support*, 7 September 2006

AFPD 10-25, *Emergency Management*, 26 September 2007

AFPD 10-26, *Counter-Chemical, Biological, Radiological, and Nuclear Operations,* 30 September 2009

AFPD 10-35, *Battlefield Airmen,* 4 February 2005

HAF Mission Directive 1-38, Deputy Chief of Staff of the Air Force (Logistics, Installations and Mission Support),5 October 2009

AFI 10-2501, *Air Force Emergency Management Program Planning and Operations*, 1 November 2010

AFI 15-128, *Air Force Weather Roles and Responsibilities,* 7 February 2011

AFI 31-101, *Integrated Defense*, 8 October 2009, Incorporating Change 1, 20 September 2010

AFMAN 31-108, *Nuclear Weapons Security Manual*, 1 February 2009

FM 3-0, *Operations*, June 2001

Adopted Forms

AF Form 847, *Recommendation for Change to Publication,* 22 September 2009

Abbreviations and Acronyms

AFDD—Air Force Doctrine Document

AFI—Air Force Instruction

AFIMS—Air Force Incident Management System

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AT—Antiterrorism

BB—Base Boundary

BDOC—Base Defense Operations Center

BSO—Battle Space Owner

BSZ—Base Security Zone

CBRN—Chemical, Biological, Radiological, Nuclear

CBRNE—Chemical, Biological, Radiological, Nuclear and High-Yield Explosive

CCIR—Commander's Critical Information Requirement

CI—Counterintelligence

COA—Course of Action

COIN—Counterinsurgency

C4ISR—Command, control, communications, computers, intelligence, surveillance and reconnaissance

DFC—Defense Force Commander

DoD—Department of Defense

DODD—Department of Defense Directive

DODI—Department of Defense Instruction

EOD—Explosive Ordnance Disposal

FISS—Foreign Intelligence Security Service

FP—Force Protection

FPCON—Force Protection Condition

FPI—Force Protection Intelligence

ID—Integrated Defense

IDP—Integrated Defense Plan

IDRMP—Integrated Defense Risk Management Process

IFC—Information Fusion Cell

IPOE—Intelligence Preparation of the Operational Environment

ISR—Intelligence Surveillance and Reconnaissance

IW—Information Warfare

LOAC—Law of Armed Conflict

METT—TC—Mission, Enemy, Troops, Terrain/Weather, Time Available, and Civilians

PSEAG—Physical Security Equipment Action Group

PIR—Priority Intelligence Requirement

PL—Protection Level

SA—Support Agreement

Terms

Air Force Incident Management System (AFIMS)—A methodology designed to incorporate the requirements of HSPD-5, the NIMS, the NRF, and OSD guidance while preserving the unique military requirements of the expeditionary Air Force. AFIMS provides the Air Force with an incident management system that is consistent with the single, comprehensive approach to domestic incident management. AFIMS provides the Air Force with the coordinating structures, processes, and protocols required to integrate its specific authorities into the collective framework of Federal departments and agencies for action to include mitigation, preparedness, response, and recovery activities. It includes a core set of concepts, principles, terminology, and technologies covering the incident command system, EOCs, incident command, training, identification, and management of resources, qualification and certification, and the collection, tracking and reporting of incident information and incident resources. The AFIMS methodology is incorporated into current operating practices through revised instructions and manuals, training products, and exercise and evaluation tools.

Antiterrorism (AT)—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (JP 1-02)

Base Boundary (BB)—Joint Publication 3-10, *Joint Security Operations in Theater*, defines the Base Boundary as a line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas. Therefore, the Base Boundary is not necessarily the base perimeter; rather, it should be established based upon the factors of Mission, Enemy, Terrain and Weather, Time, Troops available, and Civil considerations (METT-TC), specifically balancing the need of the ID forces to control key terrain with their ability to accomplish the mission. These measures decrease the likelihood of fratricide, prevent non-combatant casualties, and minimize damage to the property of friendly civilians. Boundaries may not necessarily coincide with the fenced perimeter, property lines or legal boundaries. Nevertheless, while tactical considerations will ideally determine ID boundaries, the DFC will strictly adhere to legal, jurisdictional, host nation constraints, commander‘s intent, and higher echelon orders and directives when conducting operations within the Base Boundary.

Base Defense Operations Center (BDOC)—The BDOC is the command and control center for ID operations during routine and emergency operations. The BDOC serves as the installation commander’s tactical operation center for the integrated defense effort and in that role should function as the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) integrator for ID operations.

Base Perimeter—The physical boundary of the installation.

Base Security Zone (BSZ)—The Base Security Zone is an Air Force unique concept and term to be used intra-Service only. The Air Force uses the planning term BSZ to describe the area of concern around an air base and to support the establishment and adjustment of the Base Boundary. The BSZ is the area outside the base perimeter from which the base may be

vulnerable from standoff threats (e.g., mortars, rockets, man portable air defense systems [MANPADS]). The installation commander should identify the BSZ and coordinate via their operational chain of command with local, state, federal agencies (CONUS) or host nation or area commander (OCONUS) for the BSZ to be identified as the Base Boundary. If the Base Boundary does not include all of the terrain of the BSZ, the installation commander is still responsible for either mitigating (through coordination with local, state, federal agencies [CONUS] or the area commander or host nation [OCONUS] or accepting the risks of enemy attack from the terrain outside the Base Boundary.

C-CBRN Operations—Offensive and defensive activities taken to detect, deter, disrupt, deny or destroy an adversary's CBRN capabilities and, if necessary, fight through a CBRN attack and sustain operations worldwide. The main interlinked components of C-CBRN operations are proliferation prevention, counterforce, active defense, passive defense and consequence management. (AFDD 3-40)

Commander's Critical Information Requirements (CCIRs)—CCIRs include priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs). CCIRs generate PIRs and FFIRs; the staff focuses on answering the CCIRs to support the commander's decision-making ability.

Emergency Communications Center (ECC)—The nerve center of an installation's emergency services response capability. Resources in the field communicate, often via radio, mobile data terminal, or mobile phone, with ECC controllers who then effectively manage the emergency resources for the area. These dispatch centers often use Computer Aided Dispatch (CAD) software to assist in multiple incident dispatches to keep track of all the resources within their area of responsibility. The ECC includes a central dispatch capability or its interim equivalent for the installation. It should include the minimum functions of Fire Alarm Communications Center (FACC), Base Defense Operations Center, and Medical Dispatch (as applicable).

Force Protection (FP)—The process of detecting threats and hazards to the Air Force and its mission, and applying measures to deter, pre-empt, negate or mitigate them based on an acceptable level of risk.

Force Protection Intelligence (FPI)—Analyzed, all-source information concerning threats to Department of Defense (DoD) missions, people or resources and capabilities arising from terrorists/insurgents, insiders, criminal entities, Foreign Intelligence and Security Services (FISS) and opposing military forces and environmental/medical hazards. FPI is proactive and drives FP decisions and operations. FPI is performed collaboratively by Intelligence, AFOSI, and Security Forces personnel, with cooperation and support from several other entities (i.e., operations, weather, medical, communications, etc). Intelligence supports unit deployments, readiness training, mission planning and other mission execution functions, to include, but not limited to integrated defense, the critical infrastructure program, and emergency management. In an OCONUS environment, intelligence activities are conducted on foreign adversaries. However in the CONUS, AFOSI and the local authorities are the lead for local adversaries, with intelligence providing support to their efforts.

Information Fusion Cell (IFC)—IFC is an action cell where subject matter experts (SMEs) from the Intelligence, AFOSI, Antiterrorism and Security Forces collaborate and conduct Intelligence Preparation of the Operational Environment (IPOE); the goal being to leverage information and intelligence to support the timely identification of indicators and warnings of

emerging localized threats and threats within the area of interest. The IFC and its products are the primary information sources that directly support the installation commander, the Integrated Defense Working Group and the Threat Working Group (TWG) in making proactive decisions for ID planning. The DFC must ensure information gaps identified within the IDRMP are properly identified. This is accomplished through the development of Priority Intelligence Requirements (PIRs) that are coordinated with the installation commander for inclusion into the Commander's Critical Information Requirements (CCIRs). IFC membership will be determined by the installation/higher headquarters commander.

Integrated Defense (ID)—The integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations.

Law and Order Operations—Law and Order Operations are a core capability of Air Force Security Forces. These operations include active and passive defense measures, employed across the legally-defined ground dimension of the operational environment, to mitigate potential risks and defeat adversary threats, to promote public order and efficient military operations. Law and Order Operations directly contribute to an installation's Integrated Defense. Law and Order Operations encompass many special disciplines. These include crime prevention, criminal investigations, corrections, traffic enforcement, access control and military working dogs. The specific authorities for Law and Order Operations may depend upon jurisdictional status of the installation which must be considered in planning for, and providing these Operations.

Operational Fires—Operational fires are the operational-level commander's application of nonlethal and lethal weapons effects to accomplish objectives during the conduct of a campaign or major operation.

Physical Security—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

Security—Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 1-02)